(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2002 (28.02.2002)

PCT

(10) International Publication Number
WO 02/17556 A1

(51) International Patent Classification[7]: H04L 9/32, 9/08, G06F 1/00, 13/00, 15/00

(21) International Application Number: PCT/AU01/01029

(22) International Filing Date: 20 August 2001 (20.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

PQ 9584	22 August 2000 (22.08.2000)	AU
PR 1781	29 November 2000 (29.11.2000)	AU

(71) Applicant *(for all designated States except US)*: **CMX TECHNOLOGIES PTY LTD** [AU/AU]; 78/8 Water Street, Balmain, NSW 2041 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **YOUSOFI, Siamack** [AU/AU]; 2/34 Ipima Street, Braddon, ACT 2612 (AU).

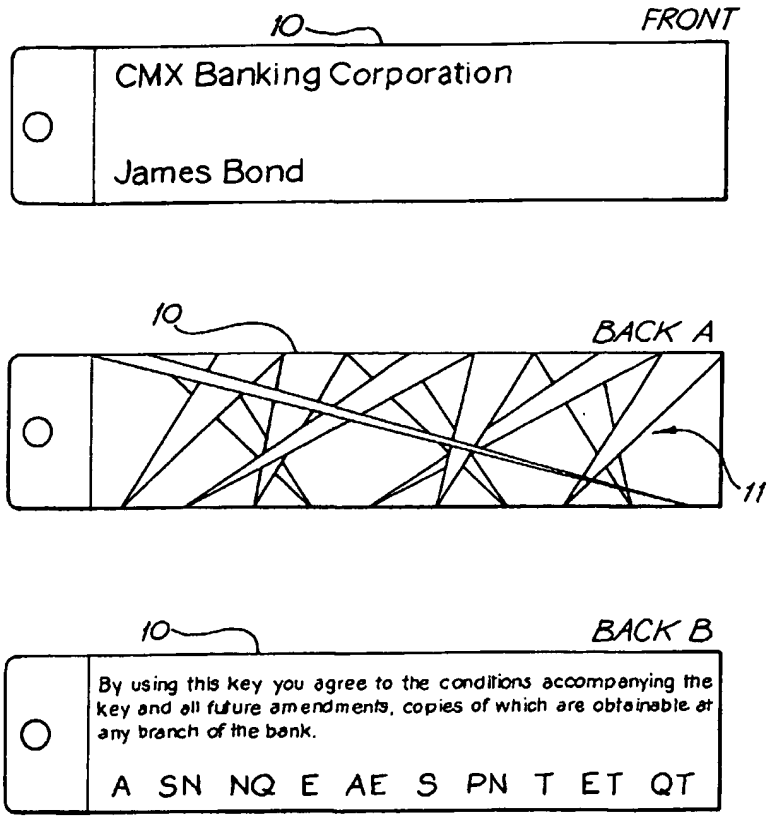
(74) Agent: **F B RICE & CO**; 605 Darling Street, Balmain NSW 2041 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: VALIDATION OF TRANSACTIONS



(57) Abstract: The invention relates to a process of validation for transactions between a user terminal and a server of the type involving: "Request, Challenge, Response, Verification and Approval". In other aspects it also relates to a computer network, server or terminal for performing the method, as well as a physical key. It involves providing a code word made up of a first series of elements to a user. Providing a key to the user to use to scramble the code word. Holding the code word and key securely at the server; Receiving a request communication at the server from a user terminal. Responding to the request by issuing a second series of elements from the server to the user terminal. Displaying the second series of elements at the terminal. Inviting the user to enter a scrambled version of the code word by selecting the elements of the first series in order from the second series and for each element selected making an entry at the terminal in dependence on the key to create a series of entries. And using the series of entries to validate the transaction.

WO 02/17556 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— *with international search report*

Title

Validation of Transactions

Technical Field

The invention relates to a process of validation for transactions between a user terminal and a server of the type involving: "Request, Challenge, Response, Verification and Approval". In other aspects it also relates to a computer network, server or terminal for performing the method, as well as a physical key.

Background Art

It is commonly accepted that at present the success or failure of consumer e-commerce depends heavily on an acceptable solution to the problem of security of online payments. Most current technologies are complex and depend heavily on strong encryption, public key infrastructures (PKI), digital certificates and digital signatures. Some other technologies such as biometrics and smart cards require specialised hardware for their implementation.

Summary of the Invention

In a first aspect the invention is a method of validation for transactions between a user terminal and a server, including the steps of:

Providing a code word made up of a first series of elements to a user.

Providing a key to the user to use to scramble the code word.

Holding the code word and key securely at the server.

Receiving a communication at the server from a user terminal (request).

Responding to the request by issuing a second series of elements from the server to the user terminal (challenge).

Displaying the second series of elements at the terminal.

Inviting the user to enter a scrambled version of the code word by selecting the elements of the first series in order from the second series and for each element selected making an entry at the terminal in dependence on the key to create a series of entries. And

Using the series of entries to validate the transaction.

The communication may take the form of a User ID entered at the terminal, and the code word may be a PIN.

The second series of elements may be a random series of elements. The elements of the sequence may simply be the ten digits 0 to 9. However, any combination of characters, symbols, digits or graphic elements can be used.

The key may include a physical body bearing visible indicia connecting pairs of points each of which is located at an internal or external edge of the body. Alternatively, the key may display, say printed, information which may appear along an edge of the key, or near apertures in the key.

The *Key* enables a user to co-relate the position of a point on a visual display to the position of a second point on the same display by holding the *Key* against the screen. The user may then capture data displayed at the second point by means of an input device. Alternatively, by aligning information printed on the key with the second series of elements displayed on the user terminal, entries may be made from the information printed on the key to select elements of the first series.

The *Key* may be of any appropriate shape and size and made of any appropriate material. For example the *Key* can be rectangular, made of paper, cardboard or plastic and be 85x21 millimetres in dimensions. Alternatively the *Key* may resemble a credit card in size and construction material.

In some cases the key may include apertures through which information on the underlying screen can be viewed. The key may also include marks which may be clicked while the key is held against the screen to make entries.

Coloured arrows on the key may help the user to first align the key with predetermined points on the screen and then click the screen co-ordinate represented by the tip of the arrow.

The arrows can vary in size, colour and shape as long as they provide a visual connection between two points, areas or objects displayed on the underlying screen. The arrows may begin and end at edges of the key, which may be external edges or edges of apertures in the key.

The communication (request) may include calibration data for the terminal generated by the user making entries depending on the size, shape or configuration of the physical body of the key. These entries may be made

by holding the key against the screen and clicking at points indicated by the key, such as at the edge of the key.

The server may use the calibration data to display the second series of elements (challenge) and a series of entry buttons at the terminal such that the key may be positioned on the terminal to link the elements of the second series with respective entry buttons.

The user may enter a scrambled version of the code word by selecting the elements of the first series in order from the second series and for each element selected clicking the respective entry button to make a series of entries.

The method may include the further steps of transmitting the series of entries made at the terminal to the server (response).

Unscrambling the entries to recover the code word, using knowledge of the second series and the key, to validate the user (verification).

Accepting or rejecting the request in dependence on the applicable business rules (approval).

The transmission of the series of entries (response) may involve transmission of the scrambled version of the code word.

After the scrambled codeword is entered and submitted the server interprets the data and verifies the codeword (verification). Depending on the applicable business rules, the server proceeds to approve or reject the transaction (approval).

Alternatively, the method may include the further steps of using the series of entries made at the terminal to encrypt a transmission to the server, and decrypting the transmission at the server.

Extra security layers in the form of electronic processes such as encryption or procedural policies may be used in addition to the steps outlined.

The invention may be used for:

- Online payments for goods and services purchased on the Internet
- Electronic Cash
- Internet Banking / Electronic Banking
- Automatic Teller Machine transactions
- EFTPOS transactions
- Security access to physical and virtual spaces
- Other similar situations.

The invention is designed to work with common Visual Display Units (VDU) used in (but not limited to) devices such as:

- Personal computers (monitors)
- Mainframe computers (terminals)
- Hand held computers
- Mobile phones
- Internet appliances
- Electronic Information Kiosks
- Interactive television sets
- Other similar devices.

The invention also requires an Input Device such as a:

- Computer mouse
- Touch pad
- Touch screen
- Stylus pen (as used in hand-held devices)
- Keyboard
- Other similar devices.

In another aspect the invention is a computer network, server or terminal for performing the method.

In a further aspect the invention is a Key comprising a physical body bearing visible indicia connecting pairs of points at an edge of the body for use in the method.

The *Key* facilitates manual scrambling or encrypting of passwords and PIN numbers. The actual process of scrambling or encryption takes place at the terminal (and involves the user's brain) but depends on the presence of the *Key* and knowledge of the User ID and PIN.

This invention can be used either independently, replacing many current security products pertaining to the Internet and other forms of online payments and fund transfers, or in conjunction with such existing products to provide additional security and accountability.

All encryption can be broken and all security measures can be defeated. Security risks can never be totally eliminated. However, over many decades and after many failures, financial institutions have developed

security measures and policies that help manage the risks by reducing them to acceptable levels. For example, PIN numbers and passwords are periodically changed or cards are captured and accounts suspended after 3 consecutive incorrect PIN entries. All of these time-tested and well-understood policies can be applied to the use of this invention.

When using the current EFT or ATM technology, we depend on three elements namely a physical card, an account number and a PIN. This invention allows us to use the same three elements on public networks such as the Internet.

Subject to correct implementation, this invention can provide the same or better level of security as the existing EFT technology without the need for expensive specialised hardware or complex software.

The *Key* has an exceptionally simple design. It can be constructed from a variety of materials including paper, cardboard, plastic, rubber, wood, or metal through simple manufacturing processes.

Unlike credit cards with magnetic strips or smart cards with built-in computer chips, this invention does not need re-encoding or re-programming and is not susceptible to electro-magnetic interference therefore extremely reliable and fail-safe.

These attributes lead to substantial manufacturing, operational and administrative cost savings.

The *Key* can be used with almost any type of Visual Display. It is even possible to use it on paper-based documents to create a confidential signature.

The *Key* can be used in a variety of circumstances ranging from Internet shopping to providing security access to buildings. New applications can be identified and implemented without the need to change the design of the *Key*.

A variety of algorithms and business rules can be implemented and continually modified and improved without the need to replace the *Key* or change its design.

Many Internet security products claim to provide a "card is present" environment. The concept of card's presence has legal significance in deciding the liabilities of the user, the merchant and the bank. This invention provides one of the strongest claims to providing "card is present" environment on the Internet.

Many instances of large-scale theft of credit card numbers used for Internet shopping have been reported in recent years and the problem is worsening due to increasing involvement of organised crime syndicates and sophistication of cyber-criminals.

Some instances involve hundreds of thousands credit card numbers. Reducing the risk requires adherence to strict security measures by all users, ISPs, merchants, banks and other service providers. The open and ad-hoc nature of the Internet limits the enforceability of such measures.

This invention employs a physical *Key* that cannot be stolen on-line. Even when physically stolen or lost the *Keys* are compromised only one at a time.

Unlike digital encryption keys (private and public), digital certificates, digital signatures, public key infrastructures (PKI) and encryption software, this invention's physical *Key* is immune from computer viruses and attacks by hackers and cyber-terrorists.

The use of this invention does not require a high level of computer literacy. For the average user it is easier to learn how to use this invention than grasp the concept of private and public encryption keys and their handling and safe keep.

This invention closely emulates EFTPOS and a "card is present" environment. Therefore, this invention may provide better compatibility with current legal framework governing on-line transactions than many alternative technologies. For the same reasons the *Key* also facilitates better allocation of responsibilities, liabilities and accountabilities.

To use the invention the user must first have possession of the *Key* and knowledge of the User ID and PIN and then physically hold the *Key* against a screen and enter values using a pointing device. A person who can fulfil all these conditions but who is not the intended legal user is less likely to reside in a far away place or able to completely cover his tracks and eliminate all clues. Therefore, the invention simplifies fraud detection and has a high forensic value. Law-enforcement agencies that currently struggle to bring cyber-criminals to justice can benefit from this invention.

Because there is no need to incorporate magnetic strips or microprocessor chips into the *Key*, it can be issued in an everlasting and durable form eliminating many instances that require card re-issue.

This invention need not render current technologies such as encryption obsolete. It can simply be used to provide an additional layer of security or extend the useful life of the underlying technology.

A further aspect of the invention is a one-time pad of disposable Keys. In this scenario the Key can be assigned a pre-defined dollar value to act as Electronic Cash or have the value defined by the user at the time of transaction to act as an Electronic Withdrawal Slip.

Brief Description of the Drawings

Examples of the invention will now be described with reference to the accompanying drawings, in which:

Fig. 1a, 1b and 1c are respectively the front and two alternative rear views of a self contained key corresponding to a first and a second type.

Fig. 2 is a view of a second type key incorporated into a credit card.

Fig. 3 is a view of a second type key incorporated into a cheque.

Fig. 4 is a screenshot illustrating a step of the Internet shopping process.

Fig. 5 is a screenshot illustrating the first step of the validation process using a first type key.

Fig. 6 is a screenshot illustrating the result of the first step of the validation process.

Fig. 7 is a screenshot illustrating the second step of the validation process using a first type key.

Fig. 8 is a screenshot illustrating the third step of the validation process using a first type key.

Fig. 9 through 12 are screenshots illustrating the steps of the validation process using a second type key.

Best Modes of the invention

Assume you have selected (or received) a Personal Identification Number; your PIN is 2016.

The sequence of digits 0 to 9 in the strip below represents a "challenge".

0	1	2	3	4	5	6	7	8	9

If you were asked to point at the digits of your PIN on this challenge strip, you would respond as follows:

0	1	2	3	4	5	6	7	8	9

2016 = 2016

Now add a second strip that includes any 10 letters of the alphabet placed adjacent to the 10 digits of our challenge strip. We can call this the "response" strip.

0	1	2	3	4	5	6	7	8	9
Q	N	S	A	H	E	X	Z	L	P

If you were asked to translate your PIN into adjacent letters using the strips above you would respond as follows.

0	1	2	3	4	5	6	7	8	9
Q	N	S	A	H	E	X	Z	L	P

2016 = SQNX

We now repeat the previous example 3 times but each time shuffle the digits in the challenge strip at random. You are still required to translate your PIN into adjacent letters.

7	0	5	2	8	4	9	3	1	6
Q	N	S	A	H	E	X	Z	L	P

2016 = ANLP

5	3	1	7	9	0	8	2	6	4
Q	N	S	A	H	E	X	Z	L	P

b_3 b_2 b_1 b_4

2016 = ZESL

0	9	3	8	4	1	5	6	2	7
Q	N	S	A	H	E	X	Z	L	P

b_2 b_3 b_4 b_1

2016 = LQEZ

Note: The elements within the response strips in all these examples remain unchanged and represent predetermined Fixed Values. (QNSAHEXZLP)

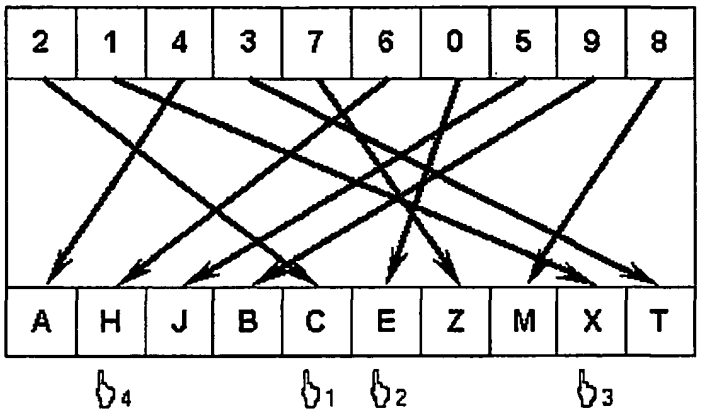
Now referring to the following diagram we shall insert a strip between the challenge and Response strips and call it the Encoder or the KEY. The encoder includes arrows that connect digits to non-adjacent letters. You use the arrows to translate your PIN into letters. (Remember to follow the arrows)

7	0	5	2	8	4	9	3	1	6
Q	N	S	A	H	E	X	Z	L	P

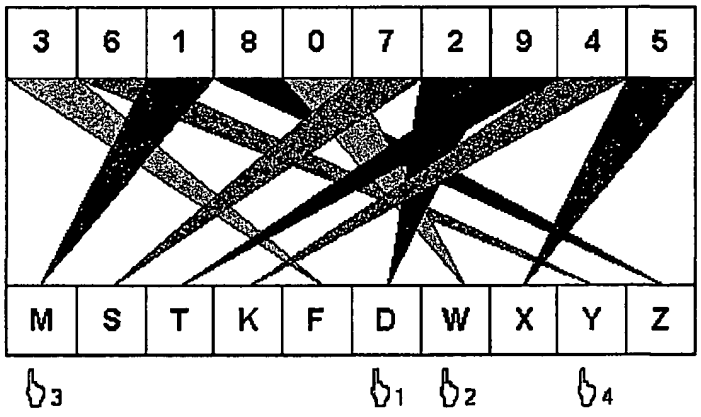
b_3 b_4 b_2 b_1

2016 = PLAZ

In the next two diagrams we repeat the previous example twice shuffling both the digits and the letters at random. We can even change any of the letters in the response strip. The orientations of the arrows on the Encoder (KEY) shall remain unchanged.



2016 = CEXH



2016 = DWMY

The elements within the response strips in these examples change at random and no longer represent predetermined fixed values. However, The arrows remain unchanged and represent Relative Positions.

In the last example the shape and color of the arrows are enhanced to provide better visual guidance.

The following examples relate to a process of validating a user's identity during online payment for goods or services purchased on the Internet using a personal computer. The process involves the steps of: "Request, Challenge, Response, Verification and Approval". The process also involves the use of a physical *Key*.

In a first example, the *Key* is rectangular, made of paper, cardboard or plastic and 85x21 millimetres in dimensions, as shown at 10 in Figs. 1a, 1b and 1c.

Alternatively, the *Key* is sized the same as a credit card and constructed of the same material, as shown at 20 in Fig. 2.

The triangular shaped areas, indicated generally at 11 on Fig. 1b represent "ARROWS" that are used to first align the card with predetermined points on a screen and then click the screen co-ordinate represented by the tip of the arrow.

The arrows 11 can vary in size, colour and shape as long as they provide a visual connection between two points, areas or objects displayed on the underlying screen.

In this example an Internet shopper visits an online store 27 and fills the shopping cart with products of choice (Fig. 4). When ready to pay for the goods, the shopper clicks an appropriate button and is presented with the screen 30 shown in Fig 5.

The financial institution issuing the card has provided the user with

- A User ID
- A *key* 10 or 20 as described above
- A password (PIN)

The first step requires the user to enter the User ID in the appropriate Textbox 31.

The second step involves holding the key 10 against the screen so that the top left corner of the card is aligned with the top left corner 32 of the ruler image as indicated by the arrow 33.

The third step involves clicking the point on screen that coincides with the bottom right corner of the physical card held against the screen as indicated by the arrow and mouse icon 34 on the image. This action will submit the User ID and the physical size of the card (in pixels) to the web server with a request for a second web page 40 (Fig 6).

The web server has a record of the User ID, user's PIN (or password) and the user's *Key* Sequence in a secure database. In addition, the server holds a series of random arrangements of ten digits (0-9) associated with the User ID and PIN.

After receiving the submitted values from step three above, the server selects one of the random arrangements of ten digits (0-9) held against the User ID and adds it to the second web page 40 in the form of a challenge strip 41 as seen in Fig. 6, sequence shown here is '1 4 6 3 2 5 9 0 8 7'. The used random sequence of digits is then deleted from the database to avoid repeated use of the same sequence.

The second web page 40 also includes a response strip 42. The letters in the response strip respond to mouse clicks by appending their value into the text-box 43 below the response strip 42.

The server will also modify the size of the rectangle 44 between the numbers and letters to match the physical size of the user's *Key* by using the pixel values transmitted from previous web page 30.

In the next step as illustrated in the screenshot 50 of Fig 7, the user must align the physical *Key* 10 in their possession in the rectangle 44 between the random sequence of digits (0-9) and the response strip 42.

Since the rectangle 44 has been sized to match the physical dimensions of the *Key* 10, the process of alignment is simple and straightforward. The process of "calibration" will work reliably for most PC monitors set at any resolution because the actual physical dimensions of users *Key* 10 is captured in the first web page 30 on the same monitor at its current settings.

When aligned, the arrows 11 will correctly connect the digits with the letters on the response strip 42.

After aligning the *Key* as illustrated in the screenshot 60 in Fig. 8, the user encodes the PIN (or password) by locating its digits on the random sequence (0-9) and following the arrows that connects each digit to respective letters on the response strip 42, clicking the letter. As the user clicks each letter its value is appended into the textbox 43 below the response strip. For instance, if the PIN contains the number '6' it can be seen to be the third number 61 in the sequence. Arrow 62 connects back to the first box 63 in response strip 42, and the user should click the letter inside box 63 to append its value in box 43. In Fig. 8 the PIN '2016' yields the encoded series 'ZQHA'.

When all the number of the PIN has been encoded the user clicks the submit button 64 to complete the transaction.

The encoded series that appear in the textbox 43 are transmitted to the server, which in turn applies the necessary logic to decode and compare them with a copy of users PIN held in its database.

If verification is successful the server applies the programmed business logic to approve or reject the transaction.

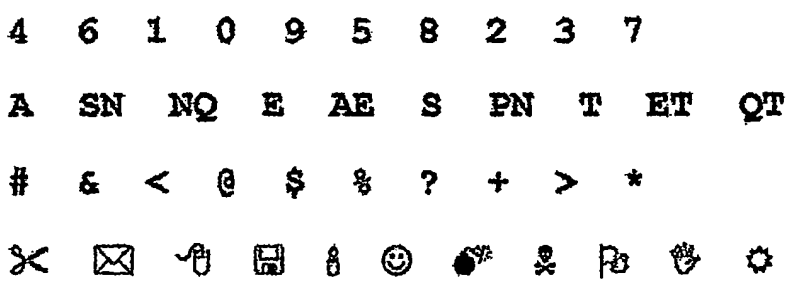
An alternative to transmitting the encoded series that appear in the textbox 43 is to use it as an encryption key for securing the shopping list and other relevant information. This method can also enhance an underlying encryption layer through the process of double encryption.

The *Key* 10 facilitates manual scrambling or encrypting of passwords and PIN numbers. The actual process of scrambling or encryption involves the user, depends on the presence of the *Key* and knowledge of the User ID and PIN.

The logical method used by the server to receive requests, issue challenges, verify responses and finally grant or withhold approval can be developed independently of the key, and can be varied to address different needs.

In general terms the server first receives a request in the form of a User ID (as well as the calibration data) and responds by presenting the user with a random sequence of displayable elements (challenge).

In the previous example the elements were simply the ten digits 0 to 9. However, any combination of characters, symbols, digits or graphic elements can be used. The *Key* is language independent and can be used with symbols and characters of any language including Chinees, Japanese, Korean (CJK) and Arabic. The number of elements can also change. Higher number of elements allows for more permutations and help to increase the security of the system. Here are some examples:



The random arrangements of the elements must avoid close similarity to minimise the risk of re-use of illegally intercepted values. A collection of ten elements can be arranged in 3,628,800 different ways (N=10!). However, many arrangements are very similar for example:

- 1 3 5 7 8 6 4 2 9 0
- 1 3 5 7 8 6 4 2 0 9
- 1 3 5 7 8 6 4 9 2 0

To avoid the risk of someone re-using an intercepted value with a closely similar permutation, the total number of permutations can be divided into smaller sets of dissimilar patterns and each set associated with a PIN. Each permutation within a set is only used once and when all combinations are used a new PIN can be issued and used with the same or a different permutation set.

Using the submitted calibration data from first web page 30 in Fig. 5, the server must arrange the elements at the correct physical size so that all the required screen elements and the user's physical *Key* can be correctly aligned.

After the PIN is entered and submitted the server interprets the data and verifies the PIN. Depending on the applicable business rules, the server proceeds to approve or reject the transaction.

If necessary the implementation can employ extra security layers in the form of electronic processes such as encryption or procedural policies.

The examples above assume that the *Key* is issued as a permanent device. However, it is possible to issue the users with a book of one-time disposable *Keys*. In this scenario the *Key* can be assigned a pre-defined dollar value to act as Electronic Cash or have the value defined by the user at the time of transaction to act a an Electronic Withdrawal Slip.

This invention is application-independent. The shape and size of the encoding device, screen representation of challenge and response elements, verification algorithm, administrative procedures such as dealing with successive wrong PIN entries and the communication methods can be varied to suit particular needs.

For example, it is possible to completely remove the merchant from the validation process by the use of digital invoices.

Any existing or new *Policy* can be employed to further enhance the security and minimise financial risks. Banks and financial institutions have existing policies that are time-tested and both operationally and legally well understood. Unlike many new Internet payment technologies, this invention can use the existing policies applicable to EFT and ATM technologies.

The simplicity, versatility and economy of the invention are reflected in the design of the two web pages that make up this demonstration. The source-code for theses two pages is included in Appendix A.

In a further example an online authentication system is designed to enhance e-commerce security. This simple system employs the method where possession (and presence) of a card and knowledge of a Personal Identification Number (PIN or password) form the basis for authentication and non-repudiation. This approach is similar to the authentication model used in EFTPOS and ATM transactions for more than two decades.

For the purpose of this example we shall assume the following:

Your name is James Bond (or Jane Bond). You are also known as The Customer.

Your financial institution is CMX Banking Corporation, also known as The Bank.

The Bank has issued you with a User ID, which is CMX007.

You have selected (or received) a Personal Identification Number. Your PIN is 2016.

In Fig. 2 an encoding strip (Key) is incorporated in a standard credit card. It includes Fixed Values.

In Fig. 3 the same encoding strip (key) can be incorporated into personal cheques or traveler's cheques 25.

This represents an alternative to incorporating Relative Position indicators (arrows) into credit cards or other instruments.

The Bank may choose to issue the KEY as a self contained device instead of physically incorporating it into other instruments. In its shape and size, the self-contained KEY can resemble physical mil-keys we use to access buildings. Fig. 1 illustrates two examples:

Option A employs Relative Position indicators (arrows) while option B incorporates Fixed Values for encoding Personal Identification Numbers.

When the encoding devices are issued in the self-contained form as in the examples above, they are directly linked to the user. Incorporating encoders into credit cards link them directly to the cards and indirectly to the user. Both methods are valid and their selection is determined by the relevant business rules.

After receiving our encoding KEY from the bank we can use it for buying goods and services on the Internet.

In the following pages actual screen shots will show how these devices can be used on the Internet.

The first step is to visit an online store and fill the shopping cart with a selection of goods. In Fig. 4 you have visited an online bookshop 27 and selected 5 books. Usually the delivery address and contact number are specified at this stage.

When ready to complete the purchase you click on a button or an icon 28 to indicate your intention to pay for the goods. Currently most secure e-commerce sites transfer the data via the Secure Socket Layer (SSL) in encrypted form. SSL is a mature technology and widely supported in browsers and web servers.

Upon receiving your request for payment, the merchant will send you the simple web page 70 shown in Fig. 9.

The screen includes a text box 71 where you enter your User ID. In this case CMX007.

The page also includes the image of a ruler 72. You are instructed to physically hold your credit card or the self-contained key against the screen. Aligning the top left corners of the card and the ruler and clicking on the position adjacent to the top right corner of your card. The ruler includes arrows and images to guide you.

Visual displays come in different physical sizes and are set at different screen resolutions. The process above is a calibration method that translates

the size of the physical card into the number of pixels on the particular visual display in use.

As soon as you click on the ruler, your User ID and the size of your card in pixels are sent to the merchant.

The merchant forwards this information to the Bank either via the Internet or through the EFTPOS network or via other appropriate links.

The Bank verifies the User ID and returns the web page 80 shown in Fig. 10 to the merchant who forwards it to you.

The page includes a strip 81 containing digits 0 to 9 in random order. The strip has the same physical width as your card.

You are instructed to physically align the KEY and the strip of numbers on the visual display as illustrated in Fig. 11. This will connect the numbers on the display with the letters of the key printed on your card.

You are required to translate your PIN into letters using the numbers on the display and letters on your card then click on the SUBMIT button 85 to complete the transaction as illustrated in Fig. 12. The letters can be entered by the use of the computer's keyboard.

The translation of your PIN is sent to the merchant who forwards it to the Bank. The Bank has a record of the encoding strip printed on your card and the challenge strips containing random numbers. After verifying that the translation of your PIN is correct the bank send a transaction approval notice to the merchant.

An alternative to transmitting the translation of your PIN to the merchant is to use it as an encryption key for securing information relevant to the bank. This method hides the bank related information from the merchant. In addition, this method can also enhance an underlying encryption layer such as SSL through the process of double encryption.

To use this system the customer must have possession of the card, have knowledge of the User ID and PIN and be present to complete the transaction.

If customers protect their physical KEY the same way they protect their credit cards and do not disclose their user ID and PIN to anyone, this system provides an environment similar to EFTPOS or ATM where the presence of a card and knowledge of PIN satisfy the authentication and non-repudiation requirements of online transactions.

This invention is application-independent. The shape and size of the encoding device, screen representation of challenge and response elements, verification algorithm, administrative procedures such as dealing with successive wrong PIN entries and the communication methods can be varied to suit particular needs.

For example, it is possible to completely remove the merchant from the validation process by the use of digital invoices.

The invention has general applications beyond e-commerce also. Access to physical spaces and general User ID / Password authentication are two examples.

Where necessary future white papers will provide additional information.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

Appendix A

The following is the actual HTML code for the two web pages featured in the previous illustration of how the *Key* can be used for Internet shopping.

CALIBERATION PAGE

```
<HTML>
<HEAD><TITLE>Example Transaction Gateway</TITLE></HEAD>
<BODY>
<form ACTION="mask"><font face="arial">
<b>First enter your USER ID . . .</b><input type="text" name="user_id" size="36">
<br><br><br><font color="blue">
<b>Then align the top left corner of your card against the ruler on the screen<br>and click on
the opposite corner as shown in the example . . .</b></font>
<br><br>
<input type=image border=0 src="ruler.gif" url="test.htm">
</form>
</BODY>
</HTML>
```

VALIDATION PAGE

```
<HTML><HEAD><TITLE>Example Transaction Gateway</TITLE>
</head>
<BODY>
<table  border cellspacing=%cellspacing% width= 266 height= 144 style="FONT-SIZE:
10pt">
<tr align="center" style="FONT-FAMILY: sans-serif">
<td width=10% height=25%>1
<td width=10%>4<td width=10%>6<td width=10%>3
<td width=10%>2<td width=10%>5<td width=10%>9
<td width=10%>0<td width=10%>8<td width=10%>7
<tr align="center">
<td colspan=10 width=10% height=50% bgcolor="white">
<font style="font-size:10pt; font-family:sans-serif,arial; font-weight:normal; color:red">
Place the key in this box<br>colour arrows facing you
<tr align="center" style="FONT-FAMILY: sans-serif">
<td width=10% height=25%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'A'">A</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'Z'">Z</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'B'">B</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'N'">N</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'T'">T</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'H'">H</a>
```

```
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'D'">D</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'P'">P</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'Q'">Q</a>
<td width=10%><a href=# onclick="document.fillform.fillin.value =
document.fillform.fillin.value + 'X'">X</a>
</table>
<br>
<form name="fillform">
<input type="text" name="fillin" size="36" READONLY><br><br>
<input type="button" value="SUBMIT">
<input type="RESET" value="RESET">
</form>
<br>
<font size=3 face="arial" color="Blue"><b>
1. Place the key on the screen between the numbers and the letters in the table above.<br>
2. From each digit of your PIN, follow the colored arrow to the connected letter and click.<br>
3. To complete the transaction press SUBMIT. (To start over press RESET)
</b></font><br><br>
<font size=3 face="arial" color="Red"><b>Never disclose your Password or PIN!</b>
</font>
</BODY>
</HTML>
```

Claims

1. A method of validation for transactions between a user terminal and a server, including the steps of:

providing a code word made up of a first series of elements to a user;

providing a key to the user to use to scramble the code word;

holding the code word and key securely at the server;

receiving a request communication at the server from a user terminal;

responding to the request by issuing a second series of elements from the server to the user terminal;

displaying the second series of elements at the terminal;

inviting the user to enter a scrambled version of the code word by selecting the elements of the first series in order from the second series and for each element selected making an entry at the terminal in dependence on the key to create a series of entries; and

using the series of entries to validate the transaction.

2. A method according to claim 1, where the request communication takes the form of a User ID entered at the terminal, and the code word is a PIN.

3. A method according to claim 1 or 2, where the second series of elements is a random series of elements.

4. A method according to claim 1, 2 or 3, where the key includes a physical body bearing visible indicia connecting pairs of points each of which is located at an internal or external edge of the body.

5. A method according to claim 4, where the scrambled version of the code word is entered by using the *Key* to co-relate the position of a point on a visual display to the position of a second point on the same display by holding the *Key* against the screen.

6. A method according to claim 4, where the request communication includes calibration data for the terminal generated by the user making entries depending on the size, shape or configuration of the physical body of the key.

7. A method according to claim 6, where the server uses the calibration data to display the second series of elements and a series of entry buttons at the terminal such that the key may be positioned on the terminal to link the elements of the second series with respective entry buttons.

8. A method according to claim 7, where the user enters a scrambled version of the code word by selecting the elements of the first series in order from the second series, and for each element selected clicking in the respective entry button to make a series of entries.

9. A method according to claim 1, 2 or 3, where the key displays information along an edge of the key, or near apertures in the key.

10. A method according to any one of claim 9, where the scrambled version of the code word is entered by aligning information displayed on the key with the second series of elements displayed on the user terminal, then making entries from the information displayed on the key to select elements of the first series.

11. A method according to any preceding claim, including the further steps of transmitting the series of entries made at the terminal to the server; unscrambling the entries at the server to recover the code word and, using knowledge of the second series and the key, to validate the user.

12. A method according to claim 11, where transmitting the series of entries involves transmitting a scrambled version of the code word.

13. A method according to any one of claims 1 to 10, including the further steps of using the series of entries made at the terminal to encrypt a transmission to the server; and decrypting the transmission at the server.

14. A computer network, server or terminal adapted for performing the method of any preceding claim.

15. A Key comprising a physical body bearing visible indicia connecting pairs of points each of which is located at an internal or external edge of the body, or, where the body displays information along an edge of the key, or near apertures in the key, the key being adapted for use in the method of any one of claims 1 to 13.

16. A one-time pad of disposable Keys according to claim 13 for use as Electronic Cash or as an Electronic Withdrawal Slip.

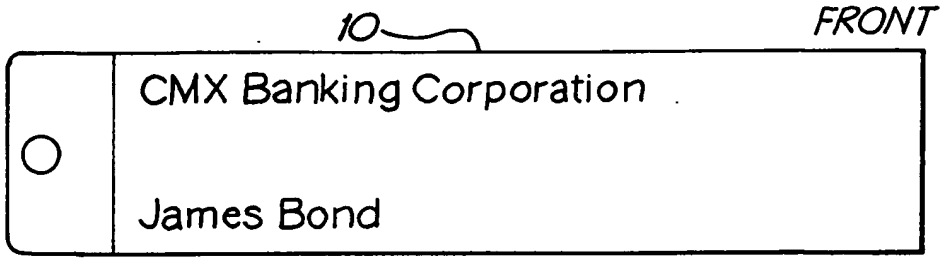


FIG. 1a

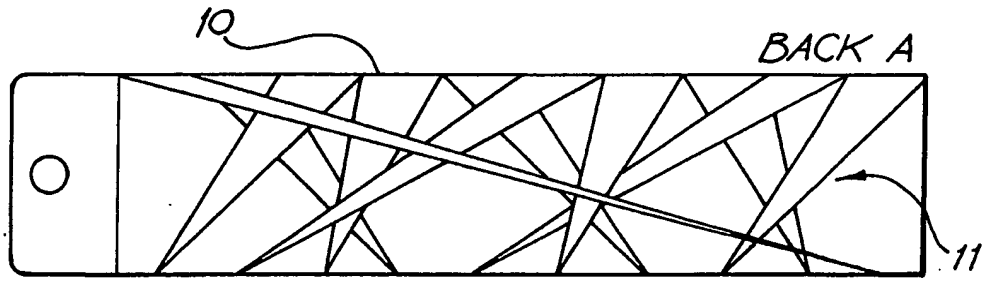


FIG. 1b

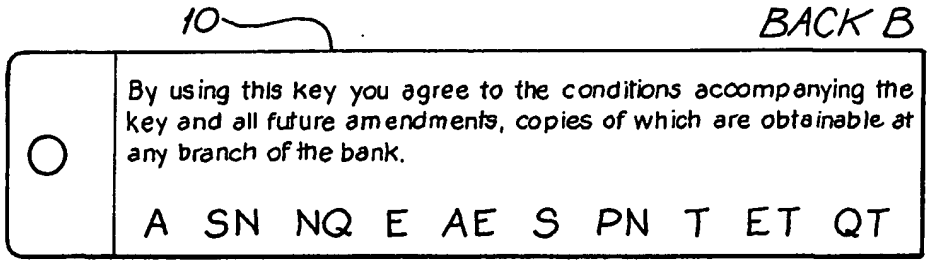


FIG. 1c

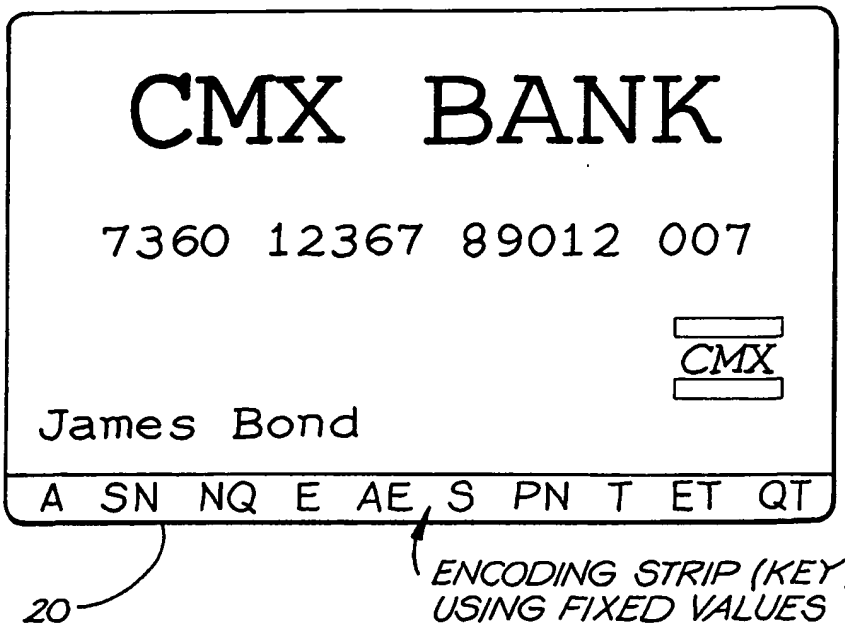

CMX BANK
7360 12367 89012 007
CMX
James Bond
A SN NQ E AE S PN T ET QT
20
ENCODING STRIP (KEY)
USING FIXED VALUES

FIG. 2

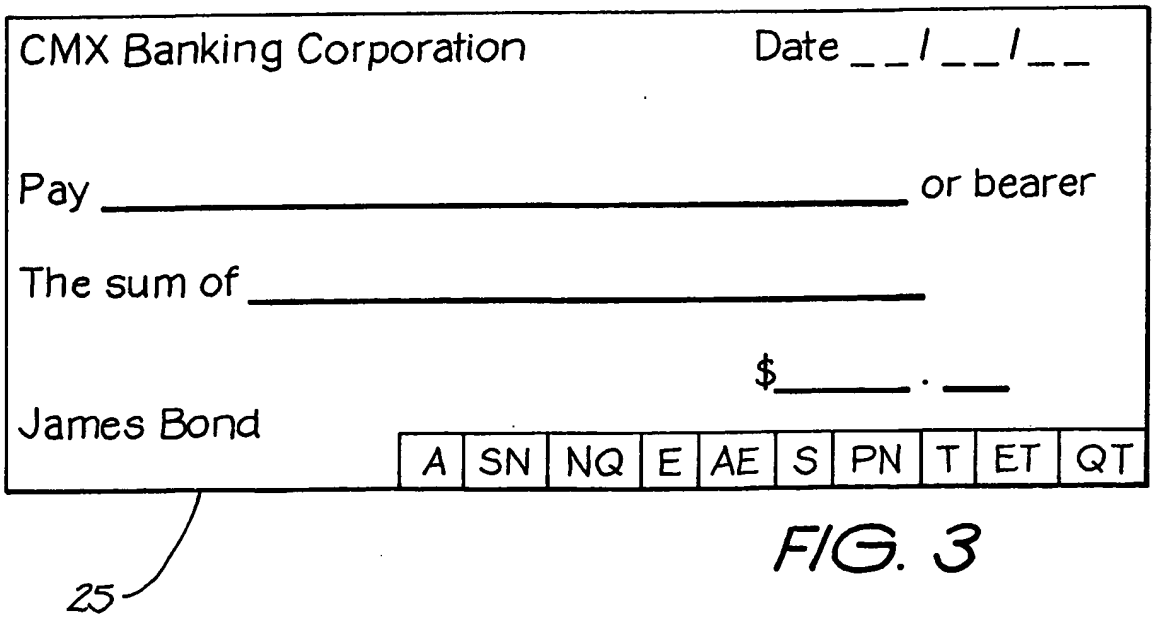

CMX Banking Corporation
Date __/__/__
Pay _____ or bearer
The sum of _____
$_____.__
James Bond
A SN NQ E AE S PN T ET QT
25

FIG. 3

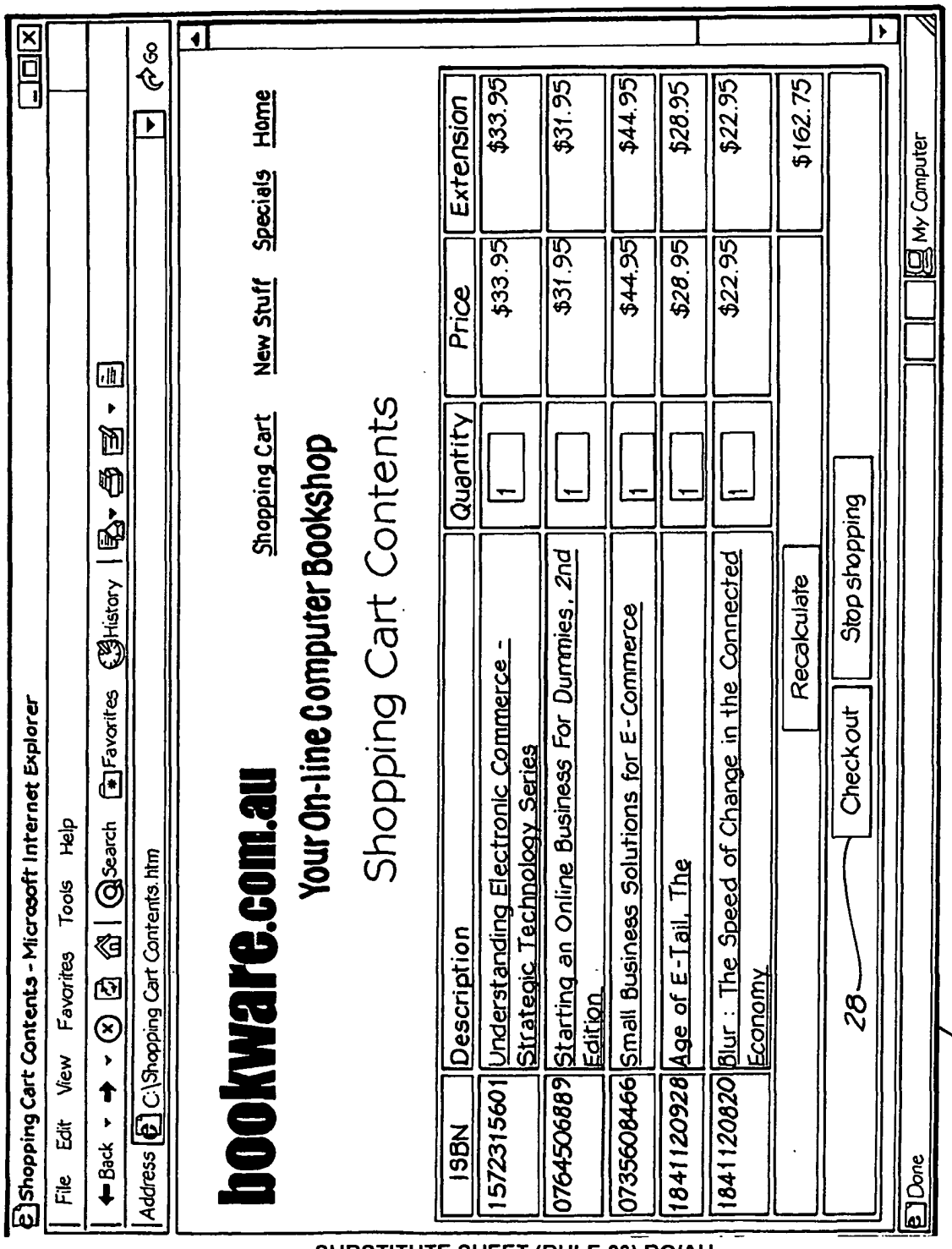

Shopping Cart Contents - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Shopping Cart Contents.htm
Go
bookware.com.au
Your On-line Computer Bookshop
Shopping Cart
New Stuff
Specials
Home
Shopping Cart Contents
ISBN
Description
Quantity
Price
Extension
1572315601
Understanding Electronic Commerce - Strategic Technology Series
1
$33.95
$33.95
0764506889
Starting an Online Business For Dummies, 2nd Edition
1
$31.95
$31.95
0735608466
Small Business Solutions for E-Commerce
1
$44.95
$44.95
1841120928
Age of E-Tail, The
1
$28.95
$28.95
1841120820
Blur : The Speed of Change in the Connected Economy
1
$22.95
$22.95
Recalculate
$162.75
Checkout
Stop shopping
28
Done
My Computer
27

FIG. 4

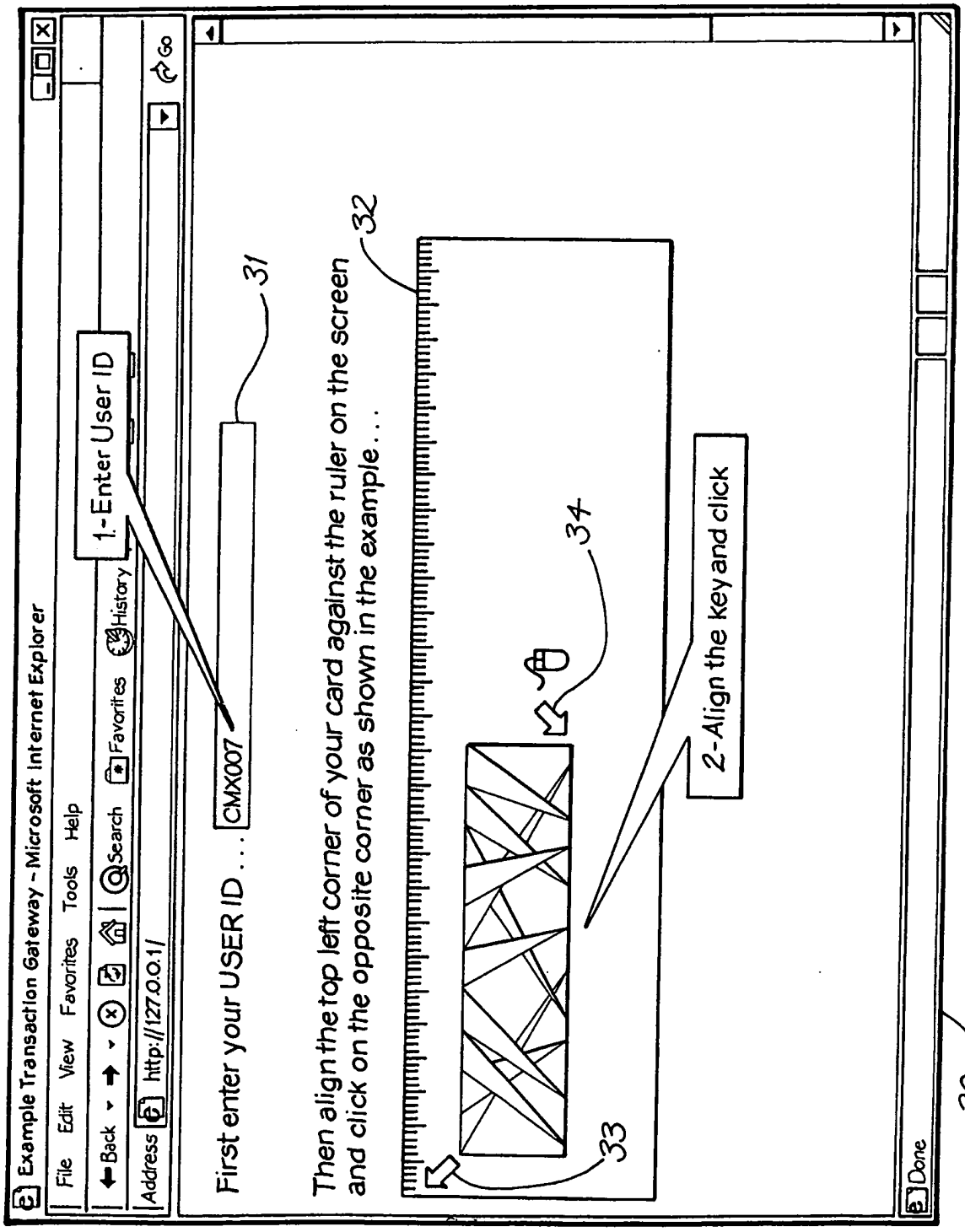

Example Transaction Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/
Go
1-Enter User ID
First enter your USER ID . . .
CMX007
31
Then align the top left corner of your card against the ruler on the screen and click on the opposite corner as shown in the example . . .
32
34
2-Align the key and click
33
30
Done

FIG. 5

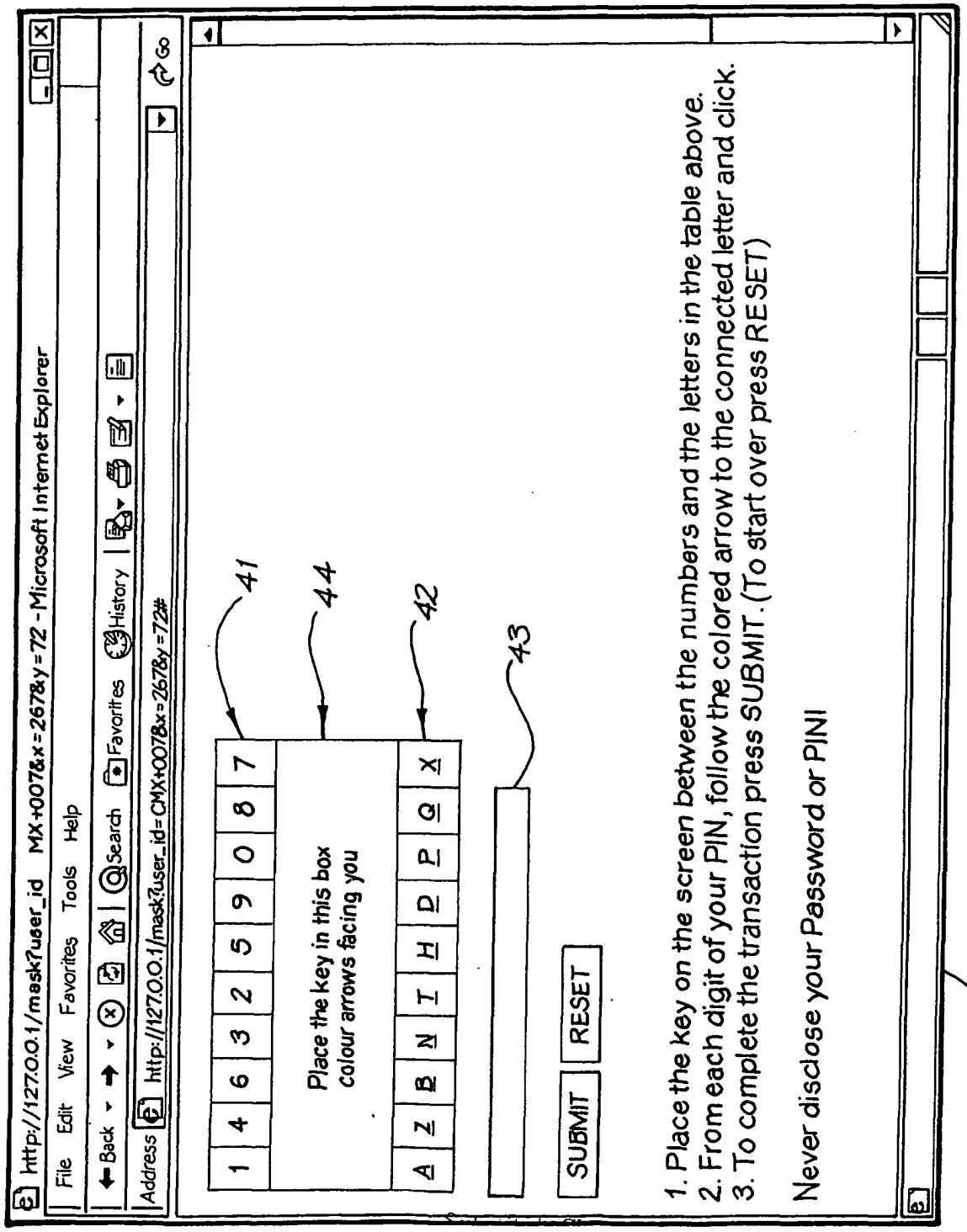

http://127.0.0.1/mask?user_id MX+007&x=267&y=72 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/mask?user_id=CMX+007&x=267&y=72#
Go
1 4 6 3 2 5 9 0 8 7
Place the key in this box colour arrows facing you
A Z B N I H D P Q X
SUBMIT RESET
41
44
42
43
40
1. Place the key on the screen between the numbers and the letters in the table above.
2. From each digit of your PIN, follow the colored arrow to the connected letter and click.
3. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your Password or PIN!

FIG. 6

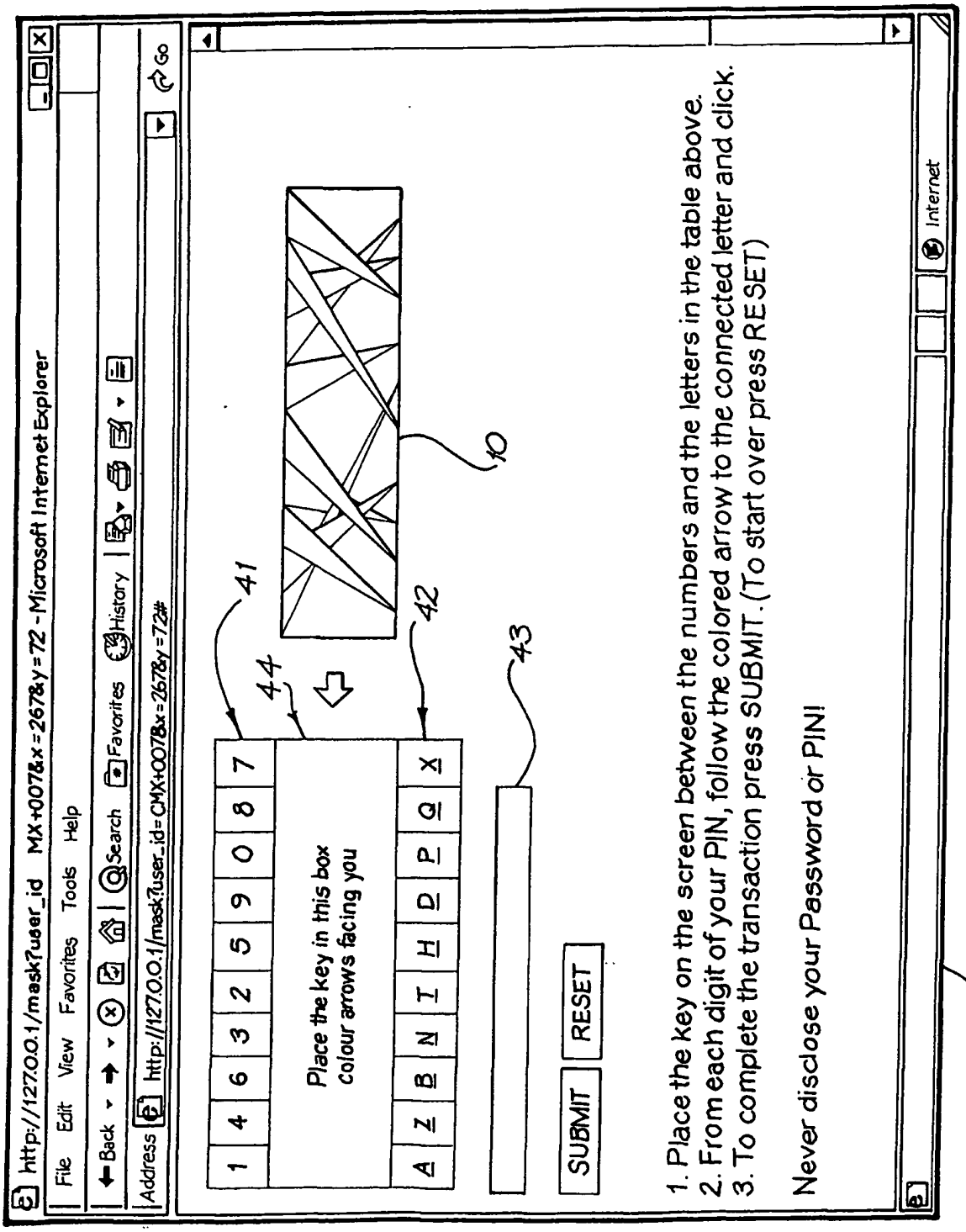

http://127.0.0.1/mask?user_id MX+0078&x=267&y=72 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/mask?user_id=CMX+0078&x=267&y=72#
Go
1 4 6 3 2 5 9 0 8 7
A Z B N I H D P Q X
Place the key in this box colour arrows facing you
41
42
43
44
10
SUBMIT
RESET
1. Place the key on the screen between the numbers and the letters in the table above.
2. From each digit of your PIN, follow the colored arrow to the connected letter and click.
3. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your Password or PIN!
Internet
50

FIG. 7

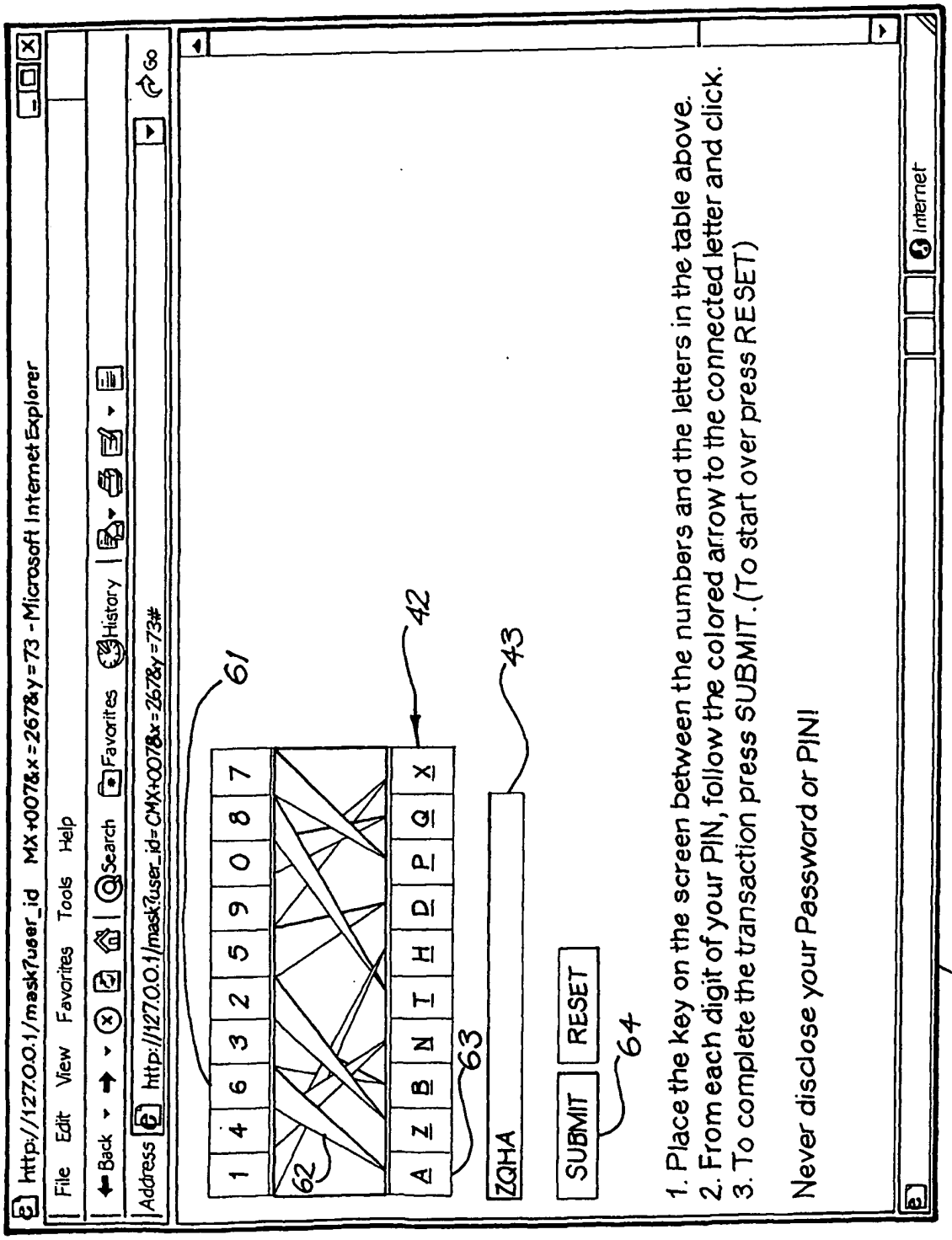

http://127.0.0.1/mask?user_id MX+007&x=267&y=73 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/mask?user_id=CMX+007&x=267&y=73#
Go
1 4 6 3 2 5 9 0 8 7
A Z B N I H D P Q X
61
62
42
63
43
ZQHA
SUBMIT
RESET
64
1. Place the key on the screen between the numbers and the letters in the table above.
2. From each digit of your PIN, follow the colored arrow to the connected letter and click.
3. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your Password or PIN!
Internet
60

FIG. 8

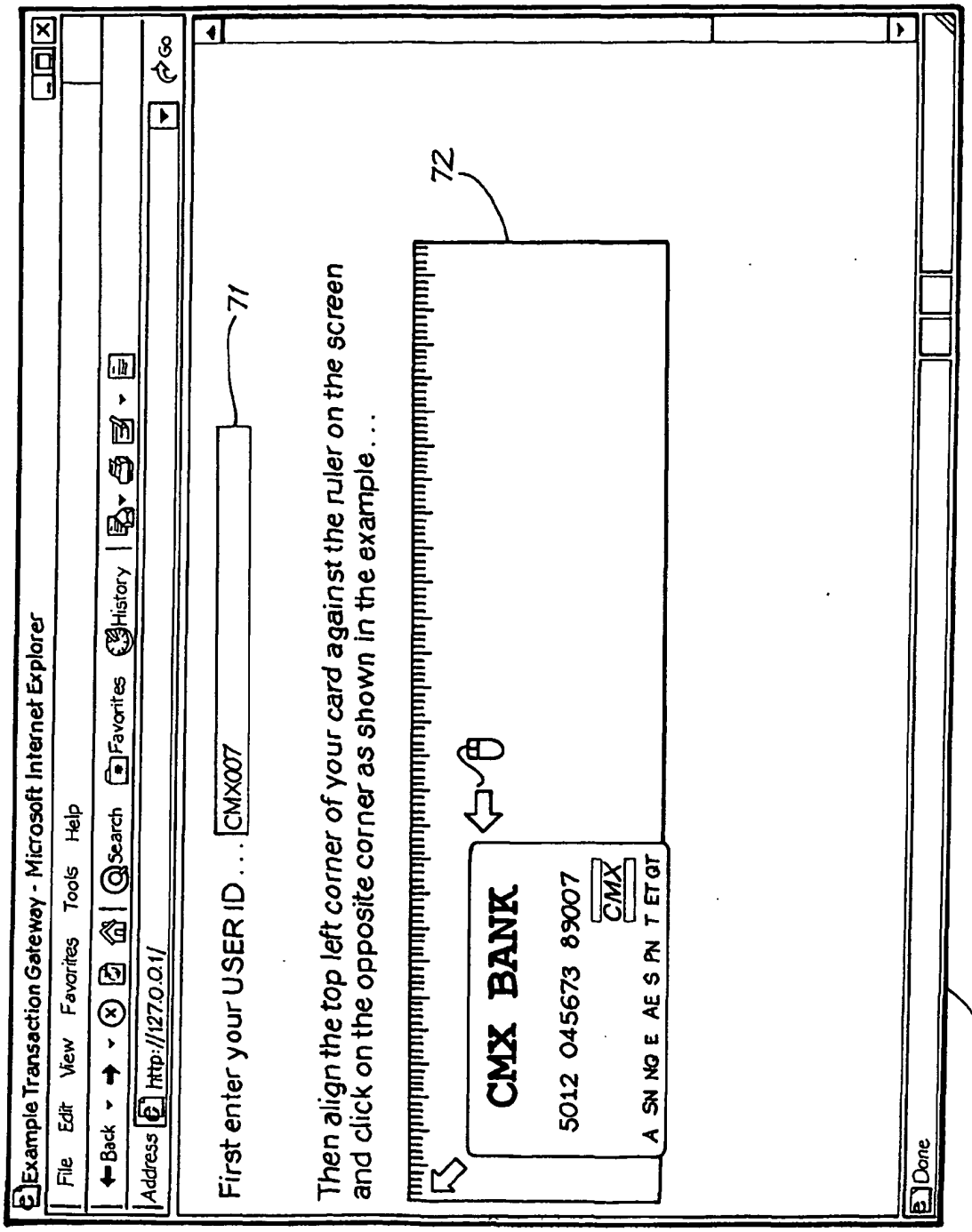

Example Transaction Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/
First enter your USER ID . . . CMX007
71
Then align the top left corner of your card against the ruler on the screen and click on the opposite corner as shown in the example . . .
72
CMX BANK
5012 045673 89007
CMX
A SN NO E AE S PN T ET QT
Done
70

FIG. 9

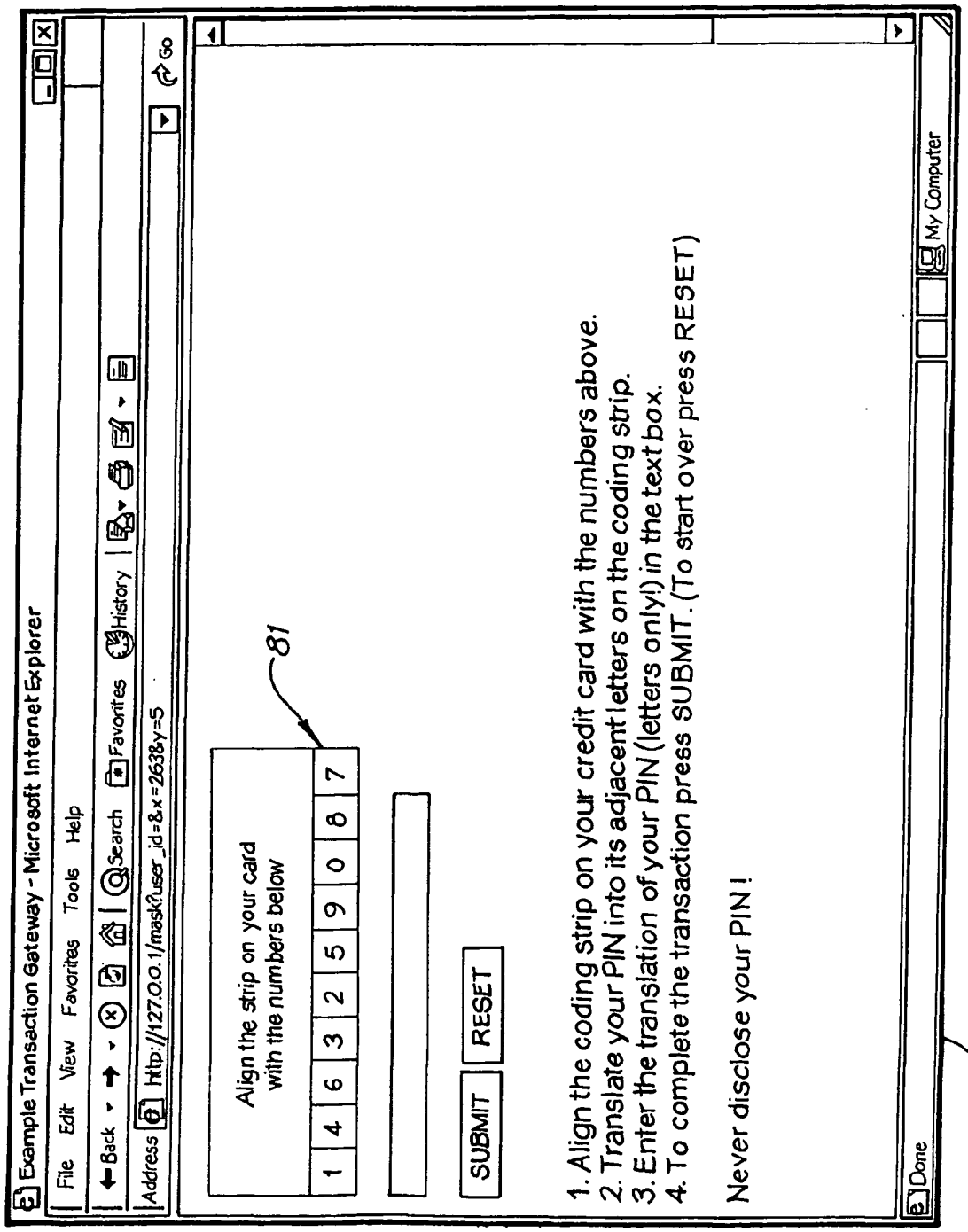

Example Transaction Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://127.0.0.1/mask?user_id=&x=2638y=5
Go
Align the strip on your card with the numbers below
81
1 4 6 3 2 5 9 0 8 7
SUBMIT
RESET
1. Align the coding strip on your credit card with the numbers above.
2. Translate your PIN into its adjacent letters on the coding strip.
3. Enter the translation of your PIN (letters only!) in the text box.
4. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your PIN!
Done
My Computer
80

FIG. 10

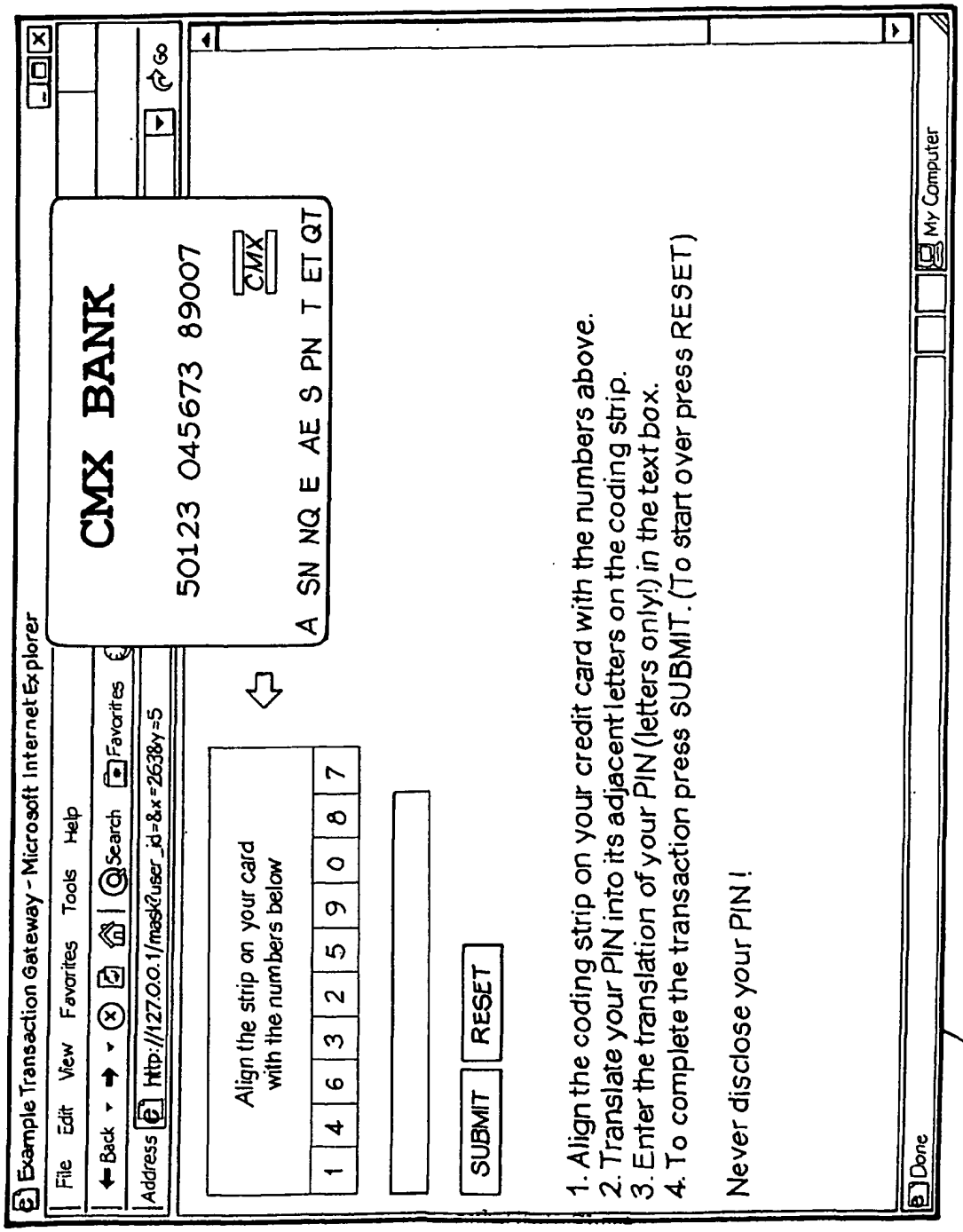

Example Transaction Gateway - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/mask?user_id=&x=2638y=5
CMX BANK
50123 045673 89007
CMX
A SN NQ E AE S PN T ET QT
Align the strip on your card with the numbers below
1 4 6 3 2 5 9 0 8 7
SUBMIT
RESET
1. Align the coding strip on your credit card with the numbers above.
2. Translate your PIN into its adjacent letters on the coding strip.
3. Enter the translation of your PIN (letters only!) in the text box.
4. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your PIN!
Done
My Computer
80

FIG. 11

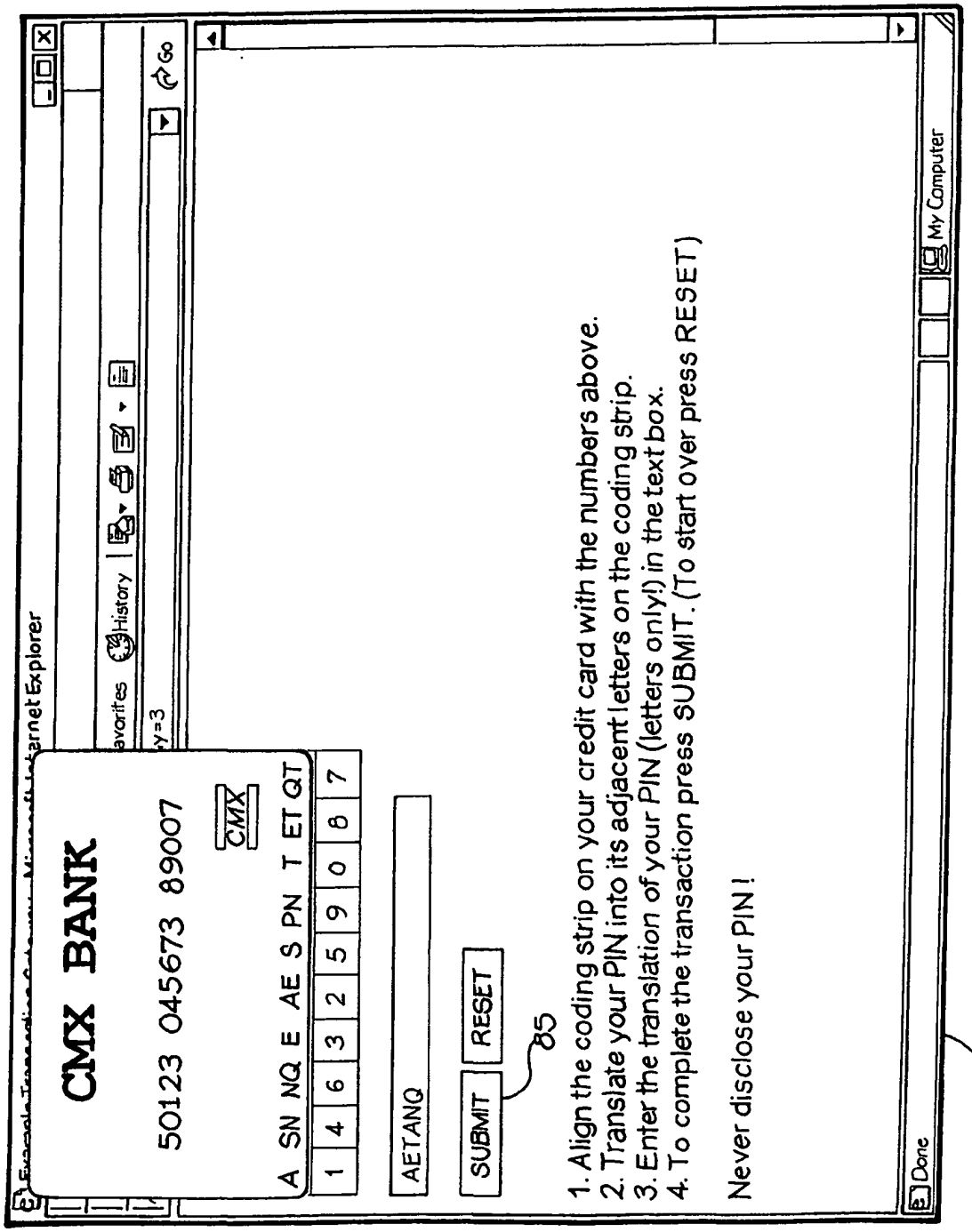

CMX BANK
50123 045673 89007
CMX
A SN NQ E AE S PN T ET QT
1 4 6 3 2 5 9 0 8 7
AETANQ
SUBMIT
RESET
85
1. Align the coding strip on your credit card with the numbers above.
2. Translate your PIN into its adjacent letters on the coding strip.
3. Enter the translation of your PIN (letters only!) in the text box.
4. To complete the transaction press SUBMIT. (To start over press RESET)
Never disclose your PIN!
Done
My Computer
80

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/01029

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: H04L 9/32, 9/08; G06F 1/00, 13/00, 15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT: Validation, authentication, transaction, code, key, scramble, encrypt, input

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,085,320 A (KALISKI, Jr.) 04 July 2000 Whole document	
A	US 6,061,790 A (BODNAR) 09 May 2000 Whole document	
A	EP 0 851 335 A2 (COMPAQ COMPUTER CORPORATION) 01 July 1998 Whole document	
A	Derwent Abstract Accession No. 98-383418/33, Class W01, JP 10154977-A (NEC SOFTWARE KOBE LTD) 09 June 1998 Abstract	

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
28 September 2001

Date of mailing of the international search report
3 OCTOBER 2001

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. (02) 6285 3929

Authorized officer
V.J. Samuel
SERINEL SAMUEL
Telephone No : (02) 6283 2382

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/01029

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
US	6085320	EP	807911	JP	11003033
US	6061790	NONE			
EP	851335	US	5953422		
JP	10154977	NONE			

END OF ANNEX